State of South Carolina Data Classification Schema

Date: September 25, 2013

Revision History

Update this table every time a new edition of the document is published

Date	Authored by	Title	Ver.	Notes
9/25/2013	Division of Information Security		1.0	Initial draft
2/10/2014	Division of Information Security		1.0	Final version – No changes from initial draft

Table of Contents

1 Executive summary

A data classification model is used to create a categorization of the State's data for efficient use and protection. Without knowing what type of data exists, who can access it, where it is located, and the value to the State, it is difficult to adequately protect data from malicious users, and develop policies and procedures to prevent the misuse of sensitive information. The data classification model is based on the following four criteria:

1. **Public:** Information intended or required for sharing with the public. Examples of public information include information provided on State web sites including meeting agendas and minutes from public meetings.
2. **Internal Use:** Non-sensitive information (e.g. job description) that is used in daily operations of an [agency]. Examples of internal use information include work phone numbers and policies, procedures, and standards and interagency communications.
3. **Confidential**: Sensitive information (e.g. birth date) in use by an [agency]. Examples of confidential information include information security plans and Personally Identifiable Information (PII).
4. **Restricted**: Highly sensitive information in use by the [agency], and is protected by statutory penalties if disclosed in an unauthorized manner. Examples of restricted information include personal health records, social security numbers (SSN), and data protected by Internal Revenue Service (IRS) Publication 1075

Please note that this schema is intended for the State of South Carolina and its agencies and institutions to act in accordance with, and for agencies and institutions to modify the brackets (i.e., [agency]) with their respective agency or institution as required.

2 Approach

The following approach was used to develop the data classification model for the State of South Carolina.

1. As part of the Task A information security risk assessments, a documentation review was performed on over one hundred and twenty-five (125) documents (i.e., policies, procedures, standards). During the documentation review, the determination was made that there are no standardized documents (i.e., policies, procedures, standards) for data classification.
2. Through analysis of the types of data present with the State's environment, it was noted that due to the range of data types (i.e. Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), PII) and regulatory compliance requirements the State would need to develop a formal methodology to classify and categorize data across agencies and implement security measures (such as encryption) accordingly. Data would need to be classified according to its sensitivity, legality and compliance requirements.
3. Several State enterprise data classification models (e.g. Minnesota, Ohio, and West Virginia) were reviewed in the development of the data classification schema. Based on the review and input from key stakeholders within the State of South Carolina, the four (4) model data classification schema (i.e. Public, Internal Use, Confidential, and Restricted) was adopted to be the foundation for data classification.
4. To determine what information goes into which schema, Federal Information Processing Standards (FIPS) 199 security objectives were used to categorize data based on its level of Confidentiality, Integrity and Availability. FIPS 199 defines three (3) levels of potential impact on organizations or individuals in the event of a breach of security (i.e., a loss of confidentiality, integrity, or availability). Please refer to Table 1 and Table 2 for additional details.

Table 1 defines data based on three security objectives for information and information systems from FIPS 199.

Table 1: FIPS 199 Security Objectives

Security Objectives	Potential Impact		
	Low	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on agency operations, agency assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on agency operations, agency assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on agency operations, agency assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on agency operations, agency assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on agency operations, agency assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on agency operations, agency assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on agency operations, agency assets, or individuals.

Table 2 uses the categorization from table one, and classifies data based on the four (4) schema data classification model.

Table 2: Data Classification Model

Data Classification Model	Confidentiality	Integrity	Availability	Example
Public	Low	Low	Low	Information on State web sites
Internal Use	Moderate	Low/Moderate	Low/Moderate	Policies, procedures, and standards
Confidential	High	Moderate/High	Moderate /High	Information security plans
Restricted[1]	High	Moderate/High	Moderate/High	Personal health information

[1] Please note that restricted and confidential information have the same security objectives; however, restricted data is protected by statutory laws, regulations, and other mandates related to protecting information.

3 Data classification

3.1 Public

Data classified as “Public” is information intended or required for sharing with the public.

Examples of public information include but are not limited to:

- Information provided on State web sites;
- Information for public distribution (e.g. state budget after public release);and
- Meeting agendas and minutes.

3.2 Internal Use

Data classified as “Internal Use” is non-confidential information that is used in daily operations of an [agency]. If internal use information is inappropriately altered, or is subject to unauthorized access, use or disclosure, little or no loss would be incurred.

Examples of internal use information include but are not limited to:

- Work phone numbers;
- Organizational charts;
- Interagency documentations; and
- Policies, procedures, and standards.

3.3 Confidential

Data classified as “Confidential” is sensitive Information in use by the [agency]. If confidential information is inappropriately altered, or is subject to unauthorized access, use or disclosure, considerable loss could occur.

Examples of confidential information include but are not limited to:

- Information security plans;
- Personally Identifiable Information (PII) information such as;[2]
    - SSN
    - Bank account information
    - Driver’s license number
- Information related to law enforcement (e.g. witness protection information); and
- Information related to minors (e.g. adoption and foster records).

[2] *PII information that is not encrypted will be considered as “Restricted” data based on South Carolina’s Data Privacy Law: Section 39-1-90,*

3.4 Restricted

Data classified as “Restricted” is highly sensitive information in use by the [agency]. If restricted Information is inappropriately altered, or is subject to unauthorized access, use or disclosure, significant loss including statutory penalties shall occur.

Examples of “restricted” information may include but are not limited to:

- IRS Publication 1075 information such as;
    - SSN received from the IRS
    - Bank account information received from the IRS
- Family Education Right and Privacy Act (FERPA) such as;
    - Tax records of parents and students
    - Grades
- Payment Card Industry (PCI) information such as; and
    - Credit card or debt card number in combination with any required security code
    - Card verification value information
- HIPAA personal health records information such as.
    - Health insurance
    - Patient treatment information

4 Appendix

4.1 Data classification references

The following sources were used in the development of the schemas for data classification:

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

NIST SP 800-60 Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

NIST SP 800-60 Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf